

Compass Security

[The ICT-Security Experts]

Smashing PLCs for Fun and Profit
[Beer Talk – Berlin – 17.02.2015]

Stephan Sekula



Compass Security
Deutschland GmbH
Tautenzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Stephan Sekula

- ✦ Seit August 2013 bei Compass als IT-Security Analyst
- ✦ Werdegang: Studium der Informatik, tätig in der Forschung; nun Sammeln von Praxiserfahrung
- ✦ Kompetenzen
 - ✦ War Dialing
 - ✦ ICS Devices

Hobbies

- ✦ Kochen & Backen
- ✦ Fahrradfahren
- ✦ Klettern
- ✦ IT-Sicherheit





Einführung

Compass Security
Deutschland GmbH
Tautenzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Automatisierung im Alltag

Fertigung



<http://www.youtube.com/watch?v=Kpvr2MVZjws&feature=plcp>



http://www.youtube.com/watch?v=YFbBVzYaH_E

Qualität Produktivität

Prozesse



Bikinger, „Raffinerie Schwechat“,
CC-Lizenz (BY 2.0)



Paul-Gerhard Koch,
„Kaprun“ Bikinger,
CC-Lizenz (BY 2.0)

kritische Infrastruktur

Gebäude



teakettle, „u1“,
CC-Lizenz (BY 2.0)



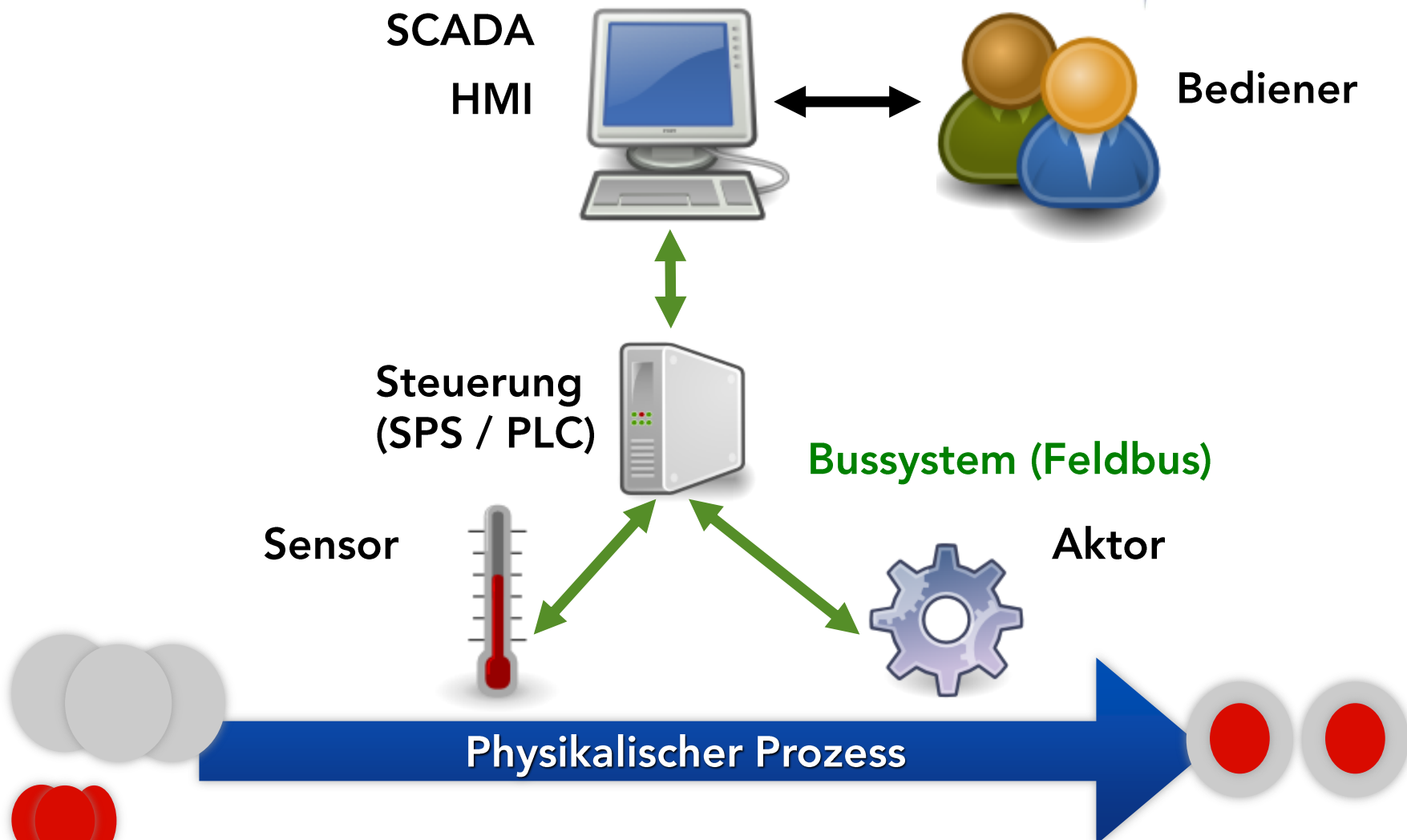
SCADACS (IRAM) – FU Berlin
(Prof. Dr.-Ing. Volker Roth)

Transport

<http://creativecommons.org/licenses/by/2.0/de/deed.de>
Alle Bilder stammen aus der kostenlosen Bilddatenbank www.piqs.de

Quelle: Ing. DI(FH) Herbert Dimberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Automatisierung in 2 min.



Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Programmable Logic Controller (PLC)



Speicherprogrammierbare Steuerung (SPS)



ICS Systeme in Europa – verwundbar (IRAM)



Quelle:
SCADACS (IRAM) – FU Berlin (Prof. Dr.-Ing. Volker Roth)



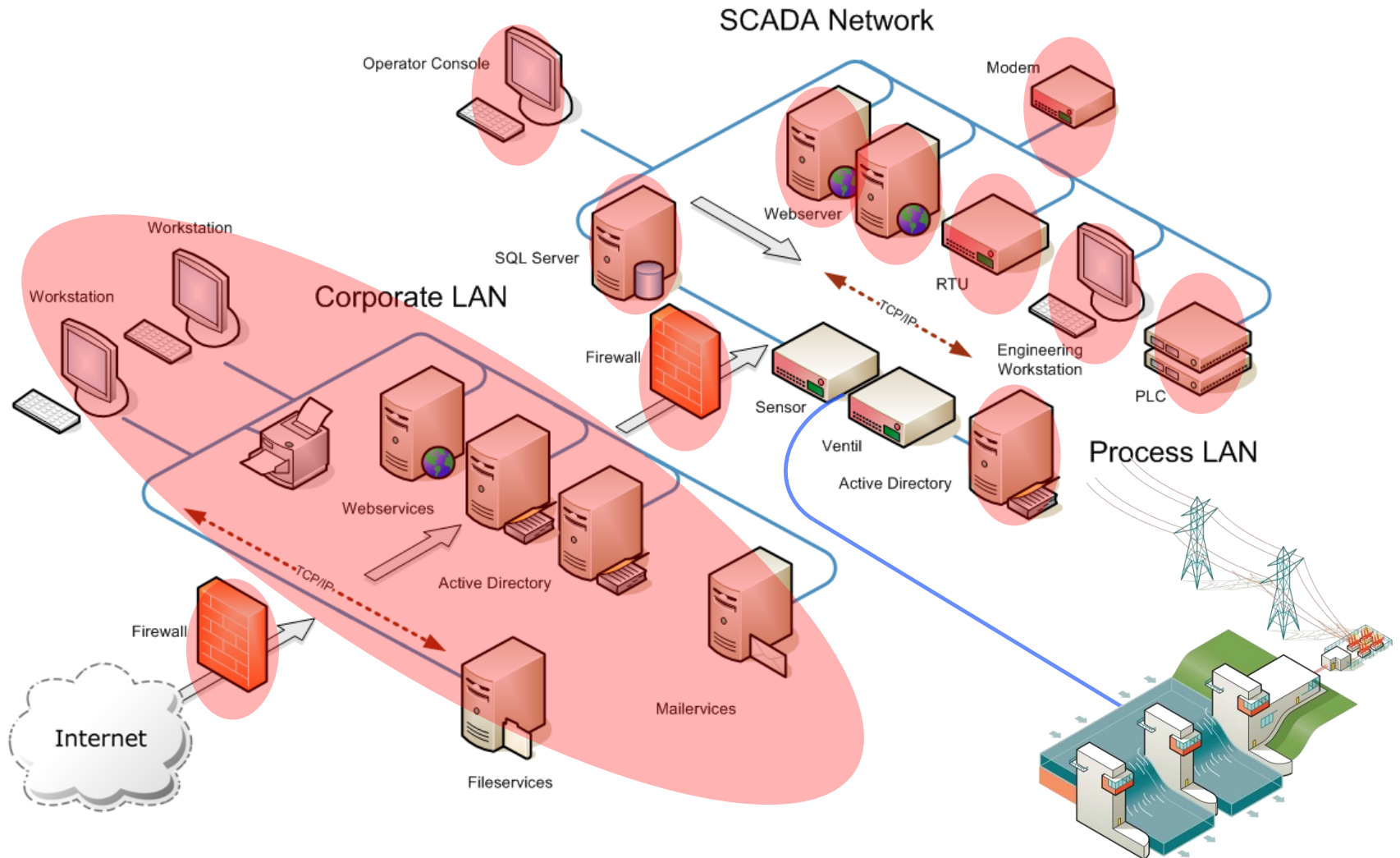
A vertical decorative image on the left side of the slide shows a magnifying glass with a wooden handle and a metal rim. The lens is focused on a yellow padlock resting on a white computer keyboard key. The background is a blurred view of other keyboard keys.

Angriffsflächen

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Ansatzpunkte möglicher Angriffe



Industrial Network Architecture

The Real World...



A vertical decorative strip on the left side of the slide features a close-up image of a computer keyboard with a yellow padlock resting on one of the keys.

Situation und Entwicklung

Compass Security
Deutschland GmbH
Tautenzienstr. 18
De-10789 Berlin

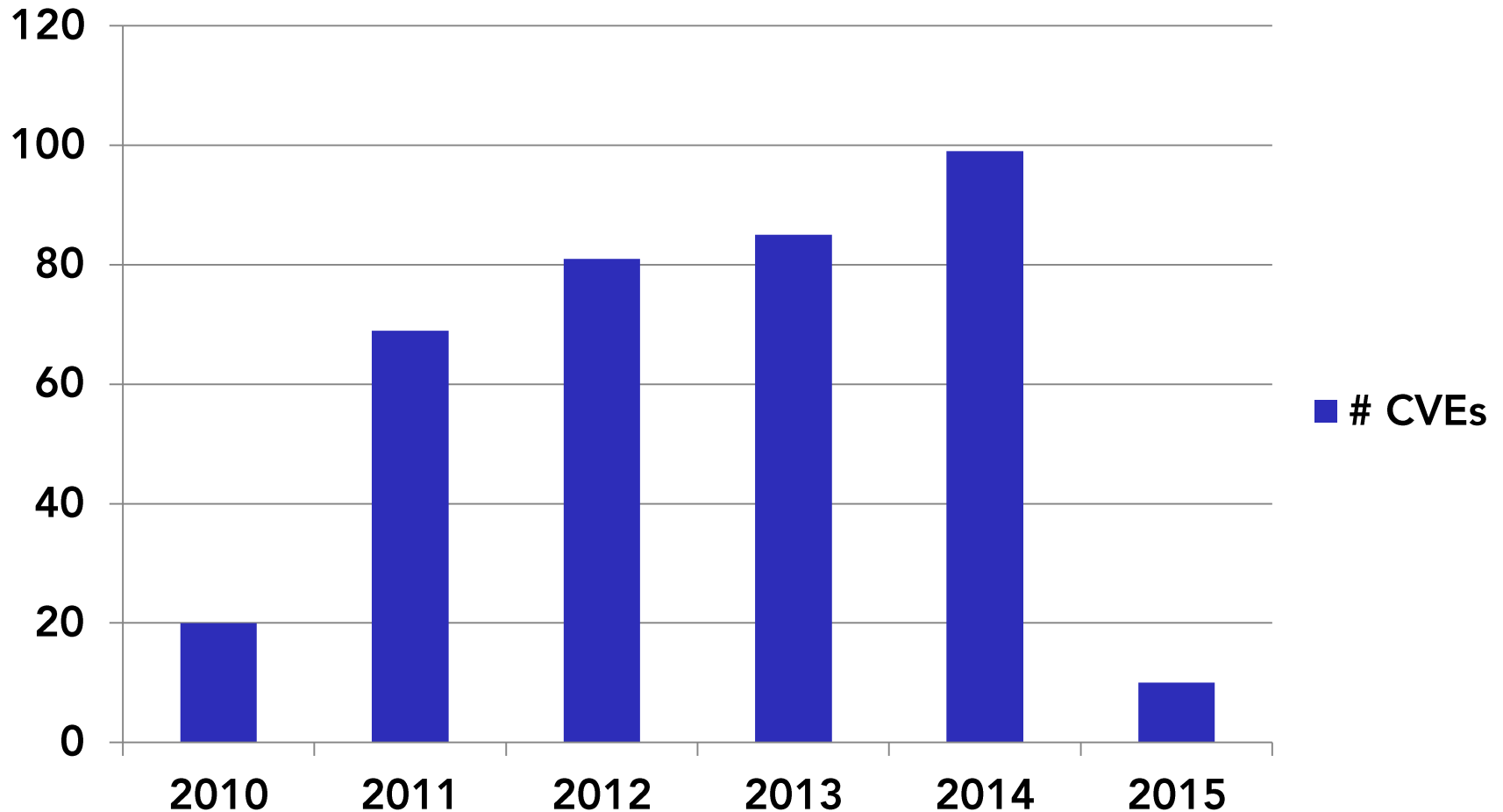
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

- ✦ Zunehmende Vernetzung
- ✦ Protokolle sind unzureichend gesichert
- ✦ Lange Lebenszeit der Systeme
- ✦ Systeme können oder werden nicht gepatcht



ICS-CERT

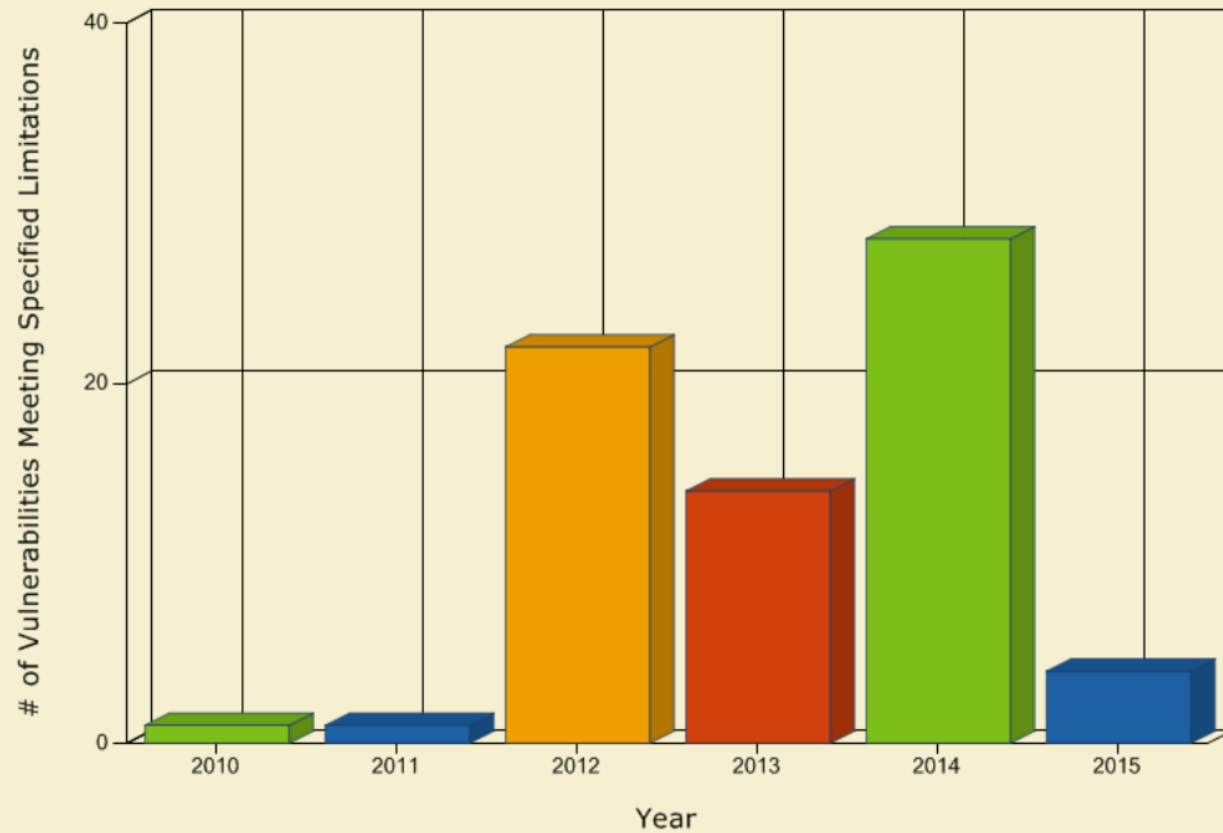
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



Search Parameters:

- Contains Software Flaws (CVE)
- Keyword (text search): simatic

Total Matches By Year



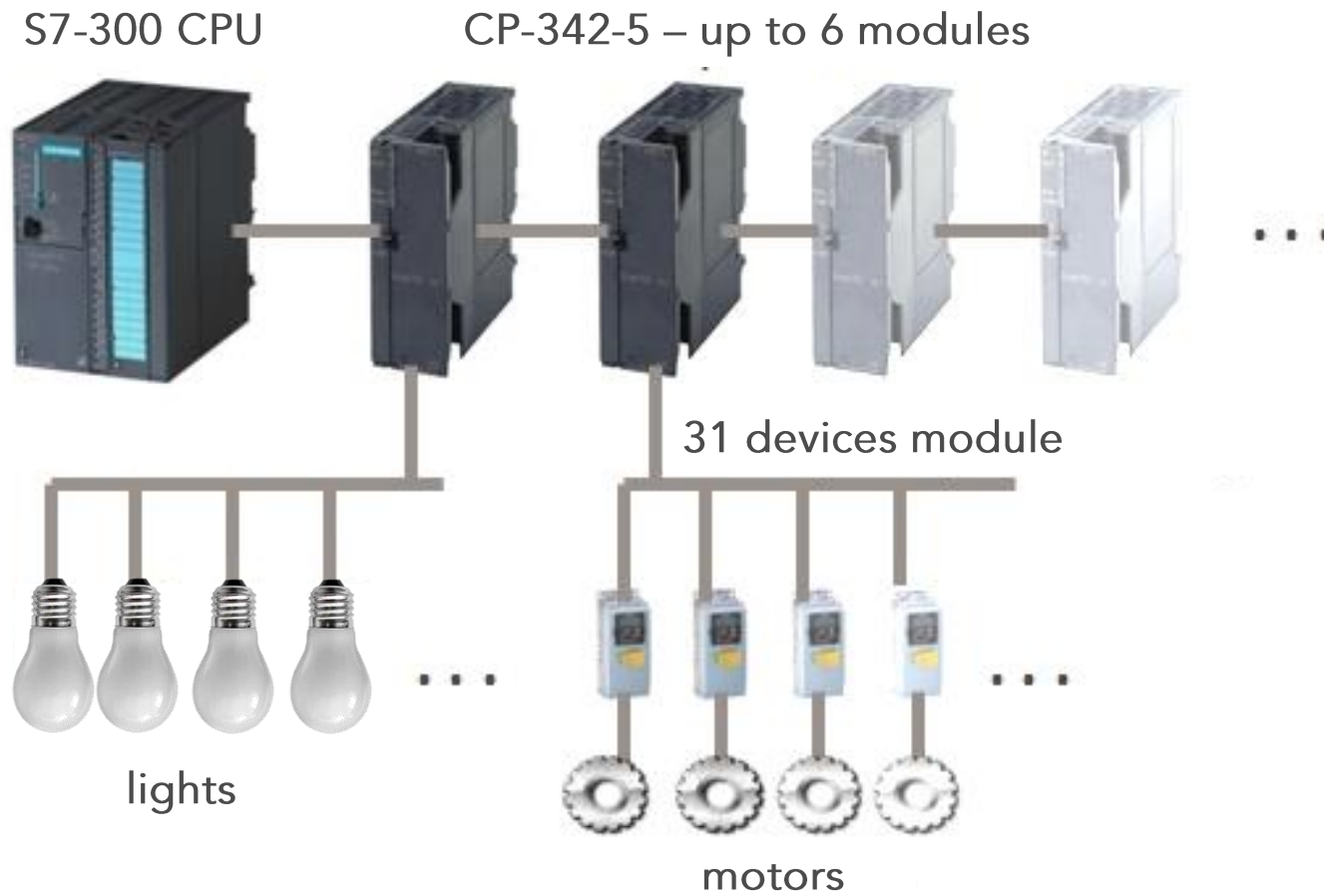
Quelle: <https://web.nvd.nist.gov/view/vuln/statistics>

A vertical decorative strip on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

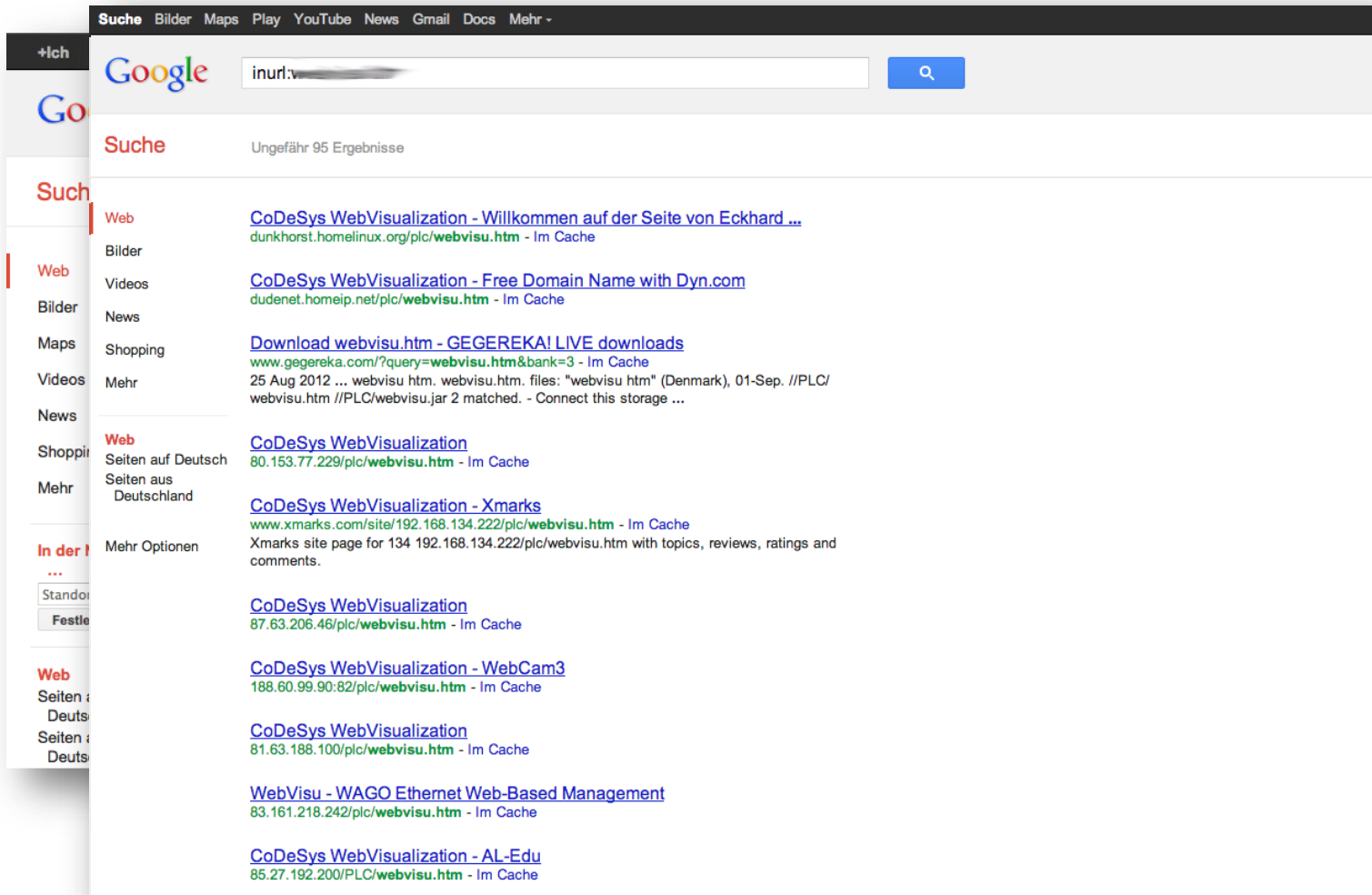
LiveDemo [Attacking Industrial Control Systems]

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de



Öffentlich zugängliche Systeme



The screenshot shows a Google search interface with the search term 'webvisu.htm' entered in the search bar. The search results are displayed in a list format, with various filters on the left side. The search results include:


- Web** [CoDeSys WebVisualization - Willkommen auf der Seite von Eckhard ...](#)
dunkhorst.homelinux.org/plc/webvisu.htm - Im Cache
- Bilder**
- Web** [CoDeSys WebVisualization - Free Domain Name with Dyn.com](#)
dudenet.homeip.net/plc/webvisu.htm - Im Cache
- Videos**
- News**
- Shopping** [Download webvisu.htm - GEGEREKA! LIVE downloads](#)
www.gegereka.com/?query=webvisu.htm&bank=3 - Im Cache
- Mehr** [25 Aug 2012 ... webvisu.htm. webvisu.htm. files: "webvisu.htm" \(Denmark\), 01-Sep. //PLC/webvisu.htm //PLC/webvisu.jar 2 matched. - Connect this storage ...](#)
- Web** [CoDeSys WebVisualization](#)
80.153.77.229/plc/webvisu.htm - Im Cache
- Web** [CoDeSys WebVisualization - Xmarks](#)
www.xmarks.com/site/192.168.134.222/plc/webvisu.htm - Im Cache
Xmarks site page for 134 192.168.134.222/plc/webvisu.htm with topics, reviews, ratings and comments.
- Web** [CoDeSys WebVisualization](#)
87.63.206.46/plc/webvisu.htm - Im Cache
- Web** [CoDeSys WebVisualization - WebCam3](#)
188.60.99.90:82/plc/webvisu.htm - Im Cache
- Web** [CoDeSys WebVisualization](#)
81.63.188.100/plc/webvisu.htm - Im Cache
- Web** [WebVisu - WAGO Ethernet Web-Based Management](#)
83.161.218.242/plc/webvisu.htm - Im Cache
- Web** [CoDeSys WebVisualization - AL-Edu](#)
85.27.192.200/PLC/webvisu.htm - Im Cache

Öffentlich zugängliche Systeme

82.55.34.62

Telecom Italia

Added on 06.11.2012

 Città Di Castello

Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. **IEC 61131-3**

host62-34-dynamic.55-82-
r.retail.telecomitalia.it

91.80.10.127

Vodafone Omnitel N.V.

Added on 19.10.2012



Inline controller with GSM/GPRS interface for coupling to other systems, with programming in acc. with **IEC 61131-3**

31.61.112.227

PTK CENTERTEL mobile data services

Added on 19.10.2012



Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. **IEC 61131-3**

85.44.179.2

Les Griffes Srl

Added on 18.10.2012



Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. **IEC 61131-3**

host2-179-static.44-85-
b.business.telecomitalia.it

188.171.255.249

Sociedad Promotora de las
Telecomunicaciones en As

Added on 18.10.2012



Inline controller with GSM/GPRS interface for coupling to other systems, with programming in acc. with **IEC 61131-3**

31.61.112.193

PTK CENTERTEL mobile data services

Added on 18.10.2012



Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. **IEC 61131-3**

92.48.157.247

Proximus Mobile Internet

Added on 03.10.2012



Inline controller with GSM/GPRS interface for coupling to other systems, with programming in acc. with **IEC 61131-3**

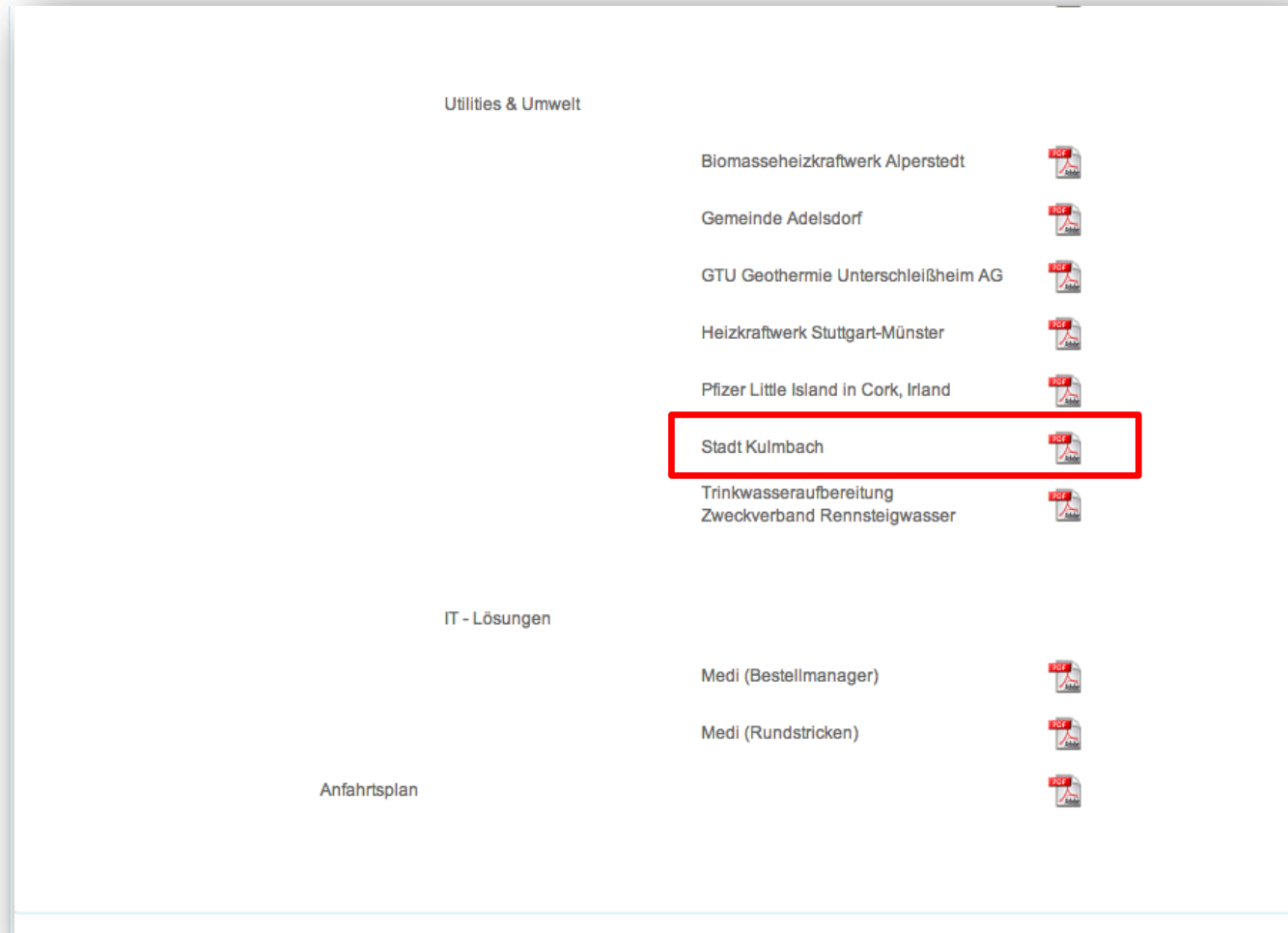
Öffentlich zugängliche Systeme

```
Terminal — bash — 132x4
mdf-macbook:plcscan mdifilippo$ python icsscan.py
Scan start...
1:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
Module : 6ES7 151-8AB00-0AB0 v.0.2
Basic Hardware : 6ES7 151-8AB00-0AB0 v.0.2
Basic Firmware : v.2.7.1
Unknown (129) : Boot Loader A
Name of the PLC :
Name of the module : IM151-8 PN/DP CPU
Plant identification :
Copyright : Original Siemens Equipment
Serial number of module : S C-X7UR74342009
Module type name : IM151-8 PN/DP CPU
Scan complete
mdf-macbook:plcscan mdifilippo$
```











Beispiele

A screenshot of a web browser displaying the SIEMENS NETLink PRO Compact interface. The page has a dark blue header with the "SIEMENS" logo on the left and a language selector set to "English" on the right. Below the header is a banner image of a green printed circuit board (PCB) with various electronic components. In the top right corner of the banner area, there is a logo for "Systeme Helmholz" with the tagline "compatible with you". A teal navigation bar contains five menu items: "Home", "Status", "Basic Configuration", "Security", and "Observe Variables". The main content area has a light gray background with the title "NETLink PRO Compact" centered. Below the title, a white box with a black border contains the text "System running: 16:35:52.990" and four blue hyperlinks: "[Status]", "[Basic Configuration]", "[Security]", and "[Observe Variables]". At the bottom of the white box is a link "[Systeme Helmholz GmbH Homepage]". On the left side of the browser window, a vertical sidebar menu is partially visible with various icons and text labels.

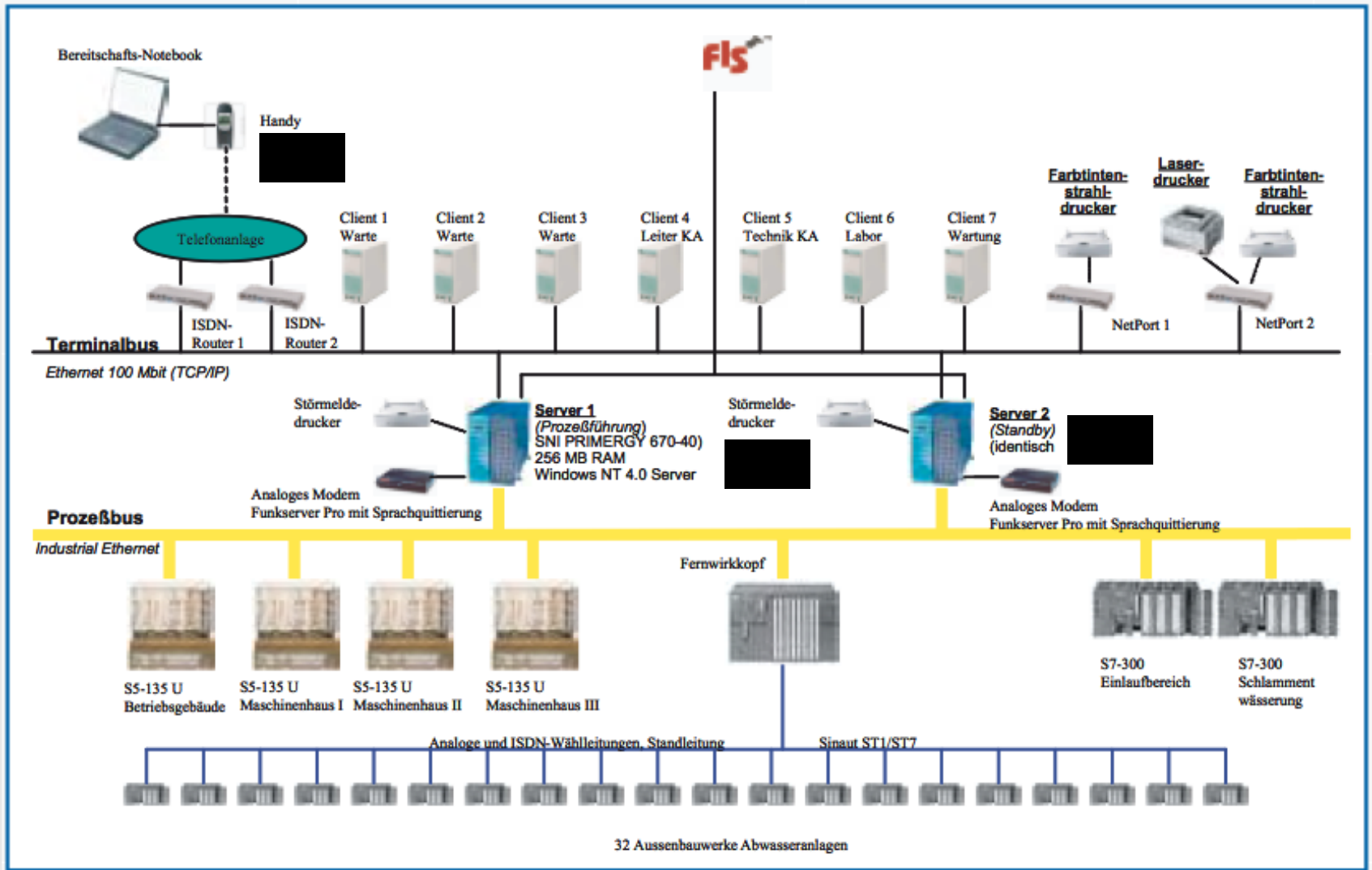
Noch einfacher....



The screenshot shows a search results page with the following content:

- Utilities & Umwelt
 - Biomasseheizkraftwerk Alperstedt 
 - Gemeinde Adelsdorf 
 - GTU Geothermie Unterschleißheim AG 
 - Heizkraftwerk Stuttgart-Münster 
 - Pfizer Little Island in Cork, Irland 
 - Stadt Kulmbach**  (highlighted with a red box)
 - Trinkwasseraufbereitung Zweckverband Rennsteigwasser 
- IT - Lösungen
 - Medi (Bestellmanager) 
 - Medi (Rundstricken) 
- Anfahrtsplan 

WarGoogling 2.0



Visualisierung als auch die Protokollierung mit den entsprechenden Daten versorgt worden.

A vertical decorative image on the left side of the slide. It shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys. The image is partially obscured by a solid blue vertical bar on the far left.

Trunk-Scanning [WarDialing]

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Ziele des WarDialing

- ✦ Identifikation des Nebenstellentyps (Sprache, Modem, FAX, ISDN Daten).
- ✦ Erkennung von Modems, Fernwartungszugängen, Einwahlsystemen, Anrufbeantwortern und FAX Servern.
- ✦ Potentiell verwundbare Systeme werden weiter analysiert.

TKSCAN Status: <Beendet> Profile: <Presentation_scan_config>

Number Selection Analysis Configuration Adapter Configuration System Configuration Scheduler [Inactive]

Pause Export -> CSV
Abort Export -> HTML

Telephone num...	Date & Time	Mode/Test	Dur...	Result	Comment
49-30-21016237	22.11.2013 18:01:47	CIP 1 speech	00:20	Possible device	Time-Out, no device answered to
49-30-21016237	22.11.2013 18:01:58	CIP 2 unrestrict...	00:11	No device	0x3492: disconnect cause from th
49-30-21016237	22.11.2013 18:02:22	FaxG3 protocol ...	00:23	Possible device	Time-Out, no device answered to
49-30-21969047	22.11.2013 18:01:35	CIP 1 speech	00:08	No device	0x3492: disconnect cause from th
49-30-21969047	22.11.2013 18:01:47	CIP 2 unrestrict...	00:11	No device	0x3492: disconnect cause from th
49-30-21969047	22.11.2013 18:02:05	FaxG3 protocol ...	00:18	Fax	+49 30 21969047
49-30-23623206	22.11.2013 18:02:14	CIP 1 speech	00:08	No device	0x3492: disconnect cause from th
49-30-23623206	22.11.2013 18:02:30	CIP 2 unrestrict...	00:16	Data device	////////////////////////////////////
49-30-23623206	22.11.2013 18:02:42	FaxG3 protocol ...	00:11	No device	0x3492: disconnect cause from th

Automat[1] Call to 49-30-23623206 finished, successful connection.
Automat[1] Recurrent calling '23623206' => forcing a pause of 3 seconds
Automat[1] Initiating a connection to 49-30-23623206 (23623206).
Automat[1] Call to 49-30-23623206 finished, no successful connection possible.
Automat[1] successful release from CAPI.
Automat[1] terminated.

Load Profile Save Profile Start Exit

Shellshock



Quellen:
www.filoo.de/blog/wp-content/uploads/2014/09/shellshock.png
openclipart.org/image/800px/svg_to_png/202367/shellshock-bug.png

Compass Security
Deutschland GmbH
Tautenzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Was ist Shellshock?



- ✦ Schwachstelle bestimmter Versionen der Bash Shell
- ✦ Befehle, die nach Funktionsdeklarationen in Umgebungsvariablen auftreten, werden ausgeführt:

```
$ env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
```

**Funktions-
deklaration**

**Sollte nicht ausgeführt werden
(kann ein beliebiger Befehl sein)**

CVEs:

CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

- ✦ Einige SPS verwenden eine (verwundbare) Version der Bash Shell
- ✦ Problem:
 - ✦ ICS Systeme erhalten kaum Sicherheitsupdates...
 - ✦ ...oder können nicht aktualisiert werden

- ✦ Keine unnötige Exponierung von ICS-Geräten ins Internet
- ✦ Einführung einer ICS-Sicherheitszone
- ✦ Fernwartung ausschließlich über VPN
- ✦ Security Audits von internen und externen Komponenten
- ✦ Risikomanagement und Self-Assessment
- ✦ Schulung von Mitarbeitern

- ✦ Wir wollen niemanden zu einer Straftat anstiften!
- ✦ Alle gezeigten Informationen dienen ausschließlich dazu, Sie zu sensibilisieren! Denn nur wer um die Gefahren weiß, kann sich davor schützen.
- ✦ Wenn Sie Fragen im Bereich IT-Sicherheit haben, sprechen Sie uns an.





Vielen Dank!



**Vielen Dank für Ihre
Aufmerksamkeit!**

Kontakt



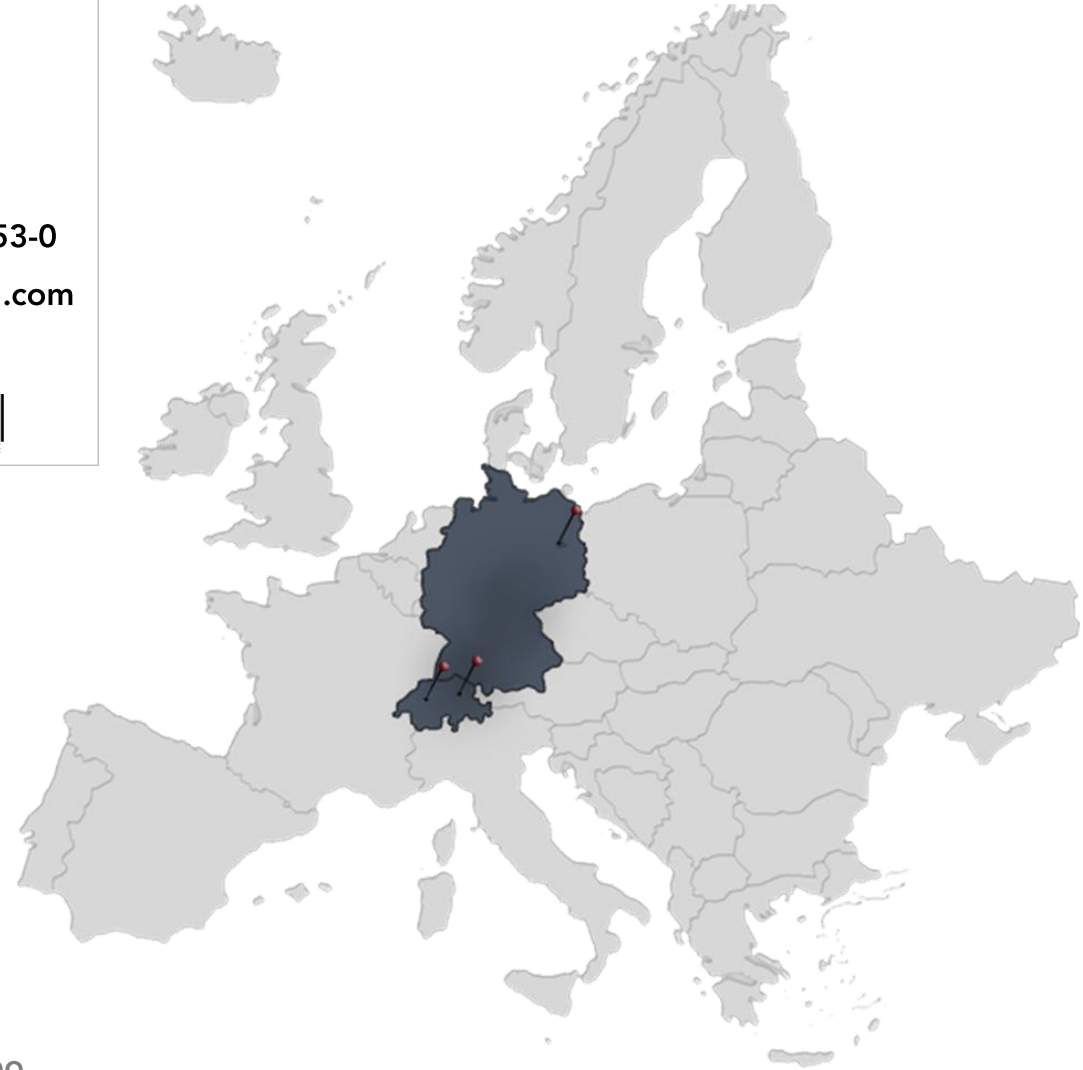
Compass Security Deutschland GmbH

Tauentzienstr. 18
10789 Berlin
Germany

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

 Secure File Exchange: www.filebox-solution.com

PGP-Fingerprint:



Slideconcept:
Review:

Marco Di Filippo
Laura-Louise Di Filippo